IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
In re application of: Charles Lingafelt et al.

Group Art Unit: 2134	:	IBM Corporation
Examiner: Norman M. Wright	:	Intellectual Property Law
Serial No.: 10/002,764	:	Dept. SHCB, Bldg. 040-3
Filed: 10/31/01	:	1701 North Street
Title: SYSTEM AND METHOD FOR DETECTING AND CONTROLLING A DRONE IMPLANTED IN A NETWORK ATTACHED DEVICE SUCH AS A COMPUTER	:	Endicott, NY 13760

U.S. Patent No.: 7,093,294 B2

Commissioner For Patents
P.O. Box 1450
Alexandria, VA 22313-1450

REQUEST FOR CERTIFICATE OF CORRECTION

Dear Sir:

In reviewing the above-identified patent, the following errors chargeable to the Official Printer, were noted (documentation attached):

In the Specification:

Column 3, line 50, change "visual's" to --vandal's-- .

Column 4, line 43, change "FIG. 12" to --FIG. 1--.

In the Claims:

Claim 7, line 20, change "a responsive" to --responsive--

Attached hereto is form PTO/SB/44. Please send the Certificate of Correction to the undersigned. Any applicable fees, please charge to Deposit Account No. 09-0457.

Respectfully submitted,

Dated: 1/17/07

By: John Pivnichny
John R. Pivnichny
Reg. No. 43,001

Telephone: (607)429-4358
Fax No: (607)429-4119

As Originally Filed

FIG. 2 shows aspects of the operation of the structure of FIG. 1.

DETAILED DESCRIPTION

The present invention provides an improved system and method for detecting the presence of a drone or zombie implanted in a network connected host device by a vandal, and controlling the output of the drone in order to prevent damage to its host or to the vandal's target.

FIG. 1 shows structural aspects of an exemplary embodiment of the present invention. In FIG. 1, a network connected device 100 is connected to a communication network such as the Internet 110. The network connected device 100 may be a computer or related device, for example a personal computer, a server, and so forth. A vandal 120 may implant a zombie or drone 105 in the network connected device 100. The purpose of the drone 105 is to launch a denial of service (DoS) attack or a portion of a distributed denial of service attack (DDoS) against a target 125, which may also be connected to the Internet 110 or other communication network.

The network connected device 100 is protected by an inbound intrusion detection system (IDS) 130, an outbound IDS 135, and a blocker 140 such as a firewall, network router, load balancer, and so forth. The outbound IDS 135 may be a special purpose device, or may be a conventional IDS similar in kind to the inbound IDS 130, but configured to observe outbound traffic rather

135, and so forth. The inbound trace log 145 and the outbound trace log 150 may be separate or combined, and may be stand-alone or included within the inbound IDS 130, the outbound IDS 135, the blocker 140, the network connected device 100, and so forth. Also, the various connections shown n FIG. 1 may be made through intermediaries without departing from the scope of the invention. For example, the inbound trace log 145 may be fed from the inbound IDS 135, or from the blocker 140, or from the network connected device 100 rather than connected directly to the Internet 110, and likewise for the outbound trace log 150.

FIG. 2 shows aspects of the method of operation of the present invention, with reference to the exemplary structure of FIG. 1. As shown in FIG. 2, the outbound IDS 135 observes outbound traffic, awaiting the appearance and detection of outbound drone traffic, such as outbound DoS or DDoS traffic from the drone 105 (step 200). Outbound drone traffic may be detected by its signature, for example according to the entries of the Common Vulnerabilities and Exposures (CVE) list sponsored by MITRE Corporation (http://www.cve.mitre.org/). When outbound drone traffic is not detected, the method continues to await the detection of outbound drone traffic (step 200).

Otherwise (i.e., outbound drone traffic is detected), the outbound IDS 135 sends a security alert to the network administrator 160 (step 205) and determines the destination address of the outbound drone traffic (step 210). The detection of outbound drone traffic and the sending of the security alert may be contingent upon more than one occurrence of a signature, as determined by

7. A system for detecting and controlling a drone implanted in a network connected device such as a computer, the system comprising:

an outbound intrusion detection system for detecting outbound denial of service traffic from a drone implanted in a network connected device and providing notice when the outbound denial of service traffic is detected;

an outbound trace log for storing a trace of outbound traffic from the network connected device;

an inbound trace log for storing a trace of inbound traffic to the network connected device;

a correlator for correlating the outbound trace log and the inbound trace log and deducing a source ID of an inbound message responsible for triggering the outbound denial of service traffic; and

a blocker, responsive to the notice provided by the outbound intrusion detection system, for blocking inbound traffic that bears the source ID and blocking the outbound denial of service traffic.

nected device, and thwarting the drone before it can damage either its host or the vandal's target.

SUMMARY

The present invention provides an improved system and method for detecting the presence of a drone or zombie implanted stealthily in a network connected host device, and controlling the output of the drone in order to prevent damage to its host or to a vandal's target.

According to the present invention, a network connected device is protected by an inbound intrusion detection system, an outbound intrusion detection system, a blocker such as a firewall, an inbound trace log for storing a trace of inbound traffic to the protected device, an outbound trace log for storing a trace of outbound traffic from the protected device, and a correlator. When the outbound intrusion detection system detects the triggering of a drone by the presence of outbound DDoS traffic, the outbound intrusion detection system instructs the blocker to block the outbound DDos traffic. The correlator then recalls the outbound trace log and the inbound trace log, correlates one log with the other, and thereby deduces a source ID of a message responsible for triggering the drone. The correlator then instructs the blocker to block any further incoming messages that bear this source ID.

Consequently, the DDoS activity of the drone may be detected, its outbound DDoS traffic may be blocked before it inflicts damage on the vandal's target, and any further triggering messages from the vandal may be intercepted and blocked before they reach the drone. These and other aspects of the invention will be more fully appreciated when considered in the light of the following detailed description and drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** shows aspects of the structure of an exemplary embodiment of the present invention.

FIG. **2** shows aspects of the operation of the structure of FIG. **1**.

DETAILED DESCRIPTION

The present invention provides an improved system and method for detecting the presence of a drone or zombie implanted in a network connected host device by a vandal, and controlling the output of the drone in order to prevent damage to its host or to the visual's target.

FIG. **1** shows structural aspects of the an exemplary embodiment of the present invention. In FIG. **1**, a network connected device **100** is connected to a communication network such as the Internet **110**. The network connected device **100** may be a computer or related device, for example a personal computer, a server, and so forth. A vandal **120** may implant a zombie or drone **105** in the network connected device **100**. The purpose of the drone **105** is to launch a denial of service (DoS) attack or a portion of a distributed denial of service attack (DDoS) against a target **125**, which may also be connected to the Internet **110** or other communication network.

The network connected device **100** is protected by an inbound intrusion detection system (IDS) **130**, an outbound IDS **135**, and a blocker **140** such as a firewall, network router, load balancer, and so forth. The outbound IDS **135** be a special purpose device, or may be a conventional IDS similar in kind to the inbound IDS **130**, but configured to observe outbound traffic rather than inbound traffic.

Inbound traffic flows from the Internet **110**, through the blocker **140**, to the network connected device **100**. Outbound traffic flows from the network connected device **100**, through the blocker **140**, to the Internet **110**. The inbound traffic may include an inbound message from the vandal **120** to the drone **105**, responsible for triggering outbound drone traffic, for example outbound denial of service (DoS or DDoS) traffic intended to attack the target **125**.

As shown in FIG. **1**, an inbound trace log **145** keeps a record of inbound traffic over a predetermined time window, and an outbound trace log **150** likewise keeps a record of outbound traffic. A correlator **155**, whose operation is described in detail below, accesses the inbound trace log **145**, the outbound trace log **150**, the inbound IDS **130**, the outbound IDS **135**, and the blocker **140**. The inbound IDS **130**, the outbound IDS **135**, and the correlator **155** may send security alerts to a network administrator **160**, which may be human, or automated, or a combination thereof.

It is important to note that the exemplary structure of the invention shown in FIG. **1** is illustrative rather than limiting. Once taught the present invention, those skilled in the art may propose other configurations equivalent to that shown in FIG. **1**. For example, the correlator **155** may be standalone logic such as a microprocessor, or may be implemented as software executed by the network connected device **100**, or by the blocker **140**, or by the inbound IDS **130**, or by the outbound IDS **135**, and so forth. The inbound trace log **145** and the outbound trace log **150** may be separate or combined, and may be stand-alone or included within the inbound IDS **130**, the outbound IDS **135**, the blocker **140**, the network connected device **100**, and so forth. Also, the various connections shown in FIG. **1** may be made through intermediaries without departing from the scope of the invention. For example, the inbound trace log **145** may be fed from the inbound IDS **135**, or from the blocker **140**, or from the network connected device **100** rather than connected directly to the Internet **110**, and likewise for the outbound trace log **150**.

FIG. **2** shows aspects of the method of operation of the present invention, with reference to the exemplary structure of FIG. **12**. As shown in FIG. **2**, the outbound IDS **135** observes outbound traffic, awaiting the appearance and detection of outbound drone traffic, such as outbound DoS or DDoS traffic from the drone **105** (step **200**). Outbound drone traffic may be detected by its signature, for example according to the entries of the Common Vulnerabilities and Exposures (CVE) list sponsored MITRE Corporation (http://www.cve.mitre.org/). When outbound drone traffic is not detected, the method continues to await the detection of outbound drone traffic (step **200**).

Otherwise (i.e., outbound drone traffic is detected), the outbound IDS **135** sends a security alert to the network administrator **160** (step **205**) and determines the destination address of the outbound drone traffic (step **210**). The detection of outbound drone traffic and the sending of the security alert may be contingent upon more than one occurrence of a signature, as determined by the parameters of the outbound IDS **135**. The outbound IDS **135** or the network administrator **160** then instructs the blocker **140** to block the outbound drone traffic (step **215**), for example by instructing the blocker **140** to block passage of outbound traffic to the destination address that represents the target **125** as determined by the outbound IDS **135** (in step **210**).

The outbound IDS **135** then provides notice of the outbound drone traffic and the destination address that repre-

sents the target **125** to the correlator **155** (step **220**). The correlator **155** fetches the inbound trace log **145** and the outbound trace log **150** (step **225**), and correlates the inbound trace log **145** with the outbound trace log **150** in order to deduce the source ID of the sender of an inbound message to the drone **105** from the vandal **120** (step **230**). Here, the term "source ID" is used broadly, and is not limited to IP addresses; rather, a source ID may also be an address derived from an IP address, an application level address or an address derived from an application level address, and so forth. This inbound message may be an inbound message from the vandal **120** responsible for triggering the outbound drone traffic from the drone **105**. The correlator **155** may perform correlation by identifying a match between various components of a signature in the CVE list mentioned earlier, or by searching the inbound trace log **145** for an inbound message that includes the address of the target **125**. This inbound message is likely to be the inbound message responsible for triggering the outbound drone traffic from the drone **105**; consequently, the source ID of this inbound message is likely to be the source ID of the vandal **120**.

The correlator **155** then sends a security alert to the network administrator **160** identifying the source ID of the vandal **120** (step **235**), and the correlator **155** or the network administrator **160** instructs the blocker **140** to block passage of any further inbound traffic that bears the source ID of the vandal **120** (step **240**). The method then returns to await detection of outbound drone traffic (step **200**). After an appropriate time, or upon cessation of outbound drone traffic, the inbound and outbound blocks may be rescinded.

From the foregoing description, those skilled in the art will appreciate that the present invention enables early detection of a drone implanted by a vandal in a network connected device, provides a way of blocking outbound drone traffic intended to harm a target device, and further provides a way to block subsequent inbound messages from the vandal intended to re-start the drone. The foregoing description is illustrative rather than limiting, however, and the present invention is limited only by the following claims.

We claim:

1. A system for detecting and controlling a drone implanted in a network connected device such as a computer, the system comprising:

an outbound intrusion detection system for detecting outbound drone traffic from a drone implanted in a network connected device and providing notice when the outbound drone traffic is detected;

a blocker for blocking the outbound drone traffic responsive to the notice provided by the outbound intrusion detection system;

an outbound trace log for storing a trace of outbound traffic from the network connected device;

an inbound trace log for storing a trace of inbound traffic to the network connected device; and

a correlator for correlating the outbound trace log and the inbound trace log and deducing a source ID of an inbound message responsible for triggering the outbound drone traffic.

2. The system of claim **1**, wherein the correlator instructs the blocker to block inbound traffic that bears the source ID.

3. The system of claim **1**, wherein the blocker is a firewall.

4. The system of claim **1**, wherein the blocker is a network router.

5. The system of claim **1**, wherein the blocker is a load balancer.

6. The system of claim **1**, wherein the outbound intrusion detection system provides a destination address of the outbound drone traffic to the correlator, and the correlator searches the incoming trace log for an inbound message that includes the destination address.

7. A system for detecting and controlling a drone implanted in a network connected device such as a computer, the system comprising:

an outbound intrusion detection system for detecting outbound denial of service traffic from a drone implanted in a network connected device and providing notice when the outbound denial of service traffic is detected;

an outbound trace log for storing a trace of outbound traffic from the network connected device;

an inbound trace log for storing a trace of inbound traffic to the network connected device;

a correlator for correlating the outbound trace log and the inbound trace log and deducing a source ID of an inbound message responsible for triggering the outbound denial of service traffic; and

a blocker, responsive to the notice provided by the outbound intrusion detection system, for blocking inbound traffic that bears the source ID and blocking the outbound denial of service traffic.

8. A system for detecting and controlling a drone implanted in a network connected device such as a computer, the system comprising:

an outbound intrusion detection system for detecting outbound denial of service traffic from a drone implanted in a network connected device, providing notice when the outbound denial of service traffic is detected, and providing a destination address of the outbound denial of service traffic;

an outbound trace log for storing a trace of outbound traffic from the network connected device;

an inbound trace log for storing a trace of inbound traffic to the network connected device;

a correlator for correlating the inbound trace log for an inbound message that includes the destination address of the outbound denial or service traffic and determining a source ID of the inbound message that includes the destination address of the outbound denial of service traffic; and

a blocker, responsive to the notice provided by the outbound intrusion detection system, for blocking inbound traffic bearing the source ID and blocking the outbound denial of service traffic.

9. A method for detecting and controlling a drone implanted in a network connected device such as a computer, the method comprising the steps of:

monitoring outbound traffic from a network connected device for outbound drone traffic; and,

when outbound drone traffic is detected, blocking the outbound drone traffic and deducing a source ID of a message responsible for triggering the outbound drone traffic by correlating an inbound trace log and an outbound trace log.

10. The method of claim **9**, further comprising the step of blocking inbound traffic that bears the source ID.

11. The method of claim **9**, wherein the outbound drone traffic is blocked by a firewall.

12. The method of claim **9**, wherein the outbound drone traffic is blocked by a network router.

13. The method of claim **9**, wherein the outbound drone traffic is blocked by a load balancer.

14. The method of claim **9**, further comprising the step of determining a destination address of the outbound drone traffic.